Presentation Title: **The Structure of Groups**

Course Title: Advanced Cryptography

Course Code: ICT-6115

Presented by :

Md. Mehedi Hasan
IT-23606
Dept. of ICT,
MBSTU

Supervised By:

Mr. Ziaur Rahman
Associate Professor
Dept. of ICT,
MBSTU

IT-23606

$\boxed{\text{① Ans}}$. Quantum computing poses a significant threat to traditional cryptographic protocols, particularly public-key crypto systems like RSA and ECC. The primary algorithm shors which can efficiently factor large-integers and solve the discrete algorithm problem in polynomial time.

The implication includes:-

i. Loss of confidentiality
ii. compromised integrity
iii. Long term security risk.

Post Quantum cryptographic Algorithms:- To counter the quantum threat, researchers are developing post-quantum cryptography algorithms that are resistant to quantum attacks.

1. Lattice based cryptography:

→ Algorithms: crystal kyber
→ Resistance: The security is based on hard lattice problems such as the learning with error problems.
→ Strengths: Efficient operations and well understand security foundations.

2. code based cryptography:

→ Algorithm: classic mceliece.
→ Resistance: Based on the difficulty of random linear codes.

IT-23606

3. Hash-based cryptography:

-> Algorithm: stateless hash based signature.

-> Resistance: Based on the security of cryptographic hash functions are resistant to quantum attacks.

-> strength: stateless design ensures security without requiring state tracking.

For instance:

-> Lattice problems remain hard even with quantum speed

-> code based cryptograph relies on an error-correcting problem that quantum computers cannot solve efficiently.

② Ans: Implementation:-

```
import time
import os
class customPRNG:
    def_init_(self, seed=None, mod=100):
        if seed is None:
            self.seed = int(time.time()*1000000)^os.getpi

        else:
            self.seed = seed
            self.mod = mod

        def next(self):
    self.seed ^=(self.seed << 13) & 0xFFFFFFFF
    self.seed ^=(self.seed >>7 ) & 0xFFFFFFFF
    self.seed ^= (self.seed << 17) & 0xFFFFFFFF
    return abs(self.seed) % self.mod
```

IT-23606

```
def random_list (self, size):
 return [self.next () for _ in range (size)]

# Example usage:
 prng = custom PRNG (mod = 1000)
 print (prng.next())
 print (prng.random_list (5))
```

③ Ans: comparison between traditional ciphers and modern symmetric ciphers:

Traditional ciphers	modern symmetric ciphers
1. Encryption speed fast.	1. fast but computationally heavier
2. Decryption speed same as encryption.	2. similar to encryption optimize for speed.
3. security weak against brute force, frequency analysis and pattern detection	3. strong again brute force and statistical attack.

strength and weakness:

Traditional ciphers:

① Caesar ciphers:

strength: simple and easy to implement.

weakness: only 25 possible keys, vulnerable to frequency analysis.

JT-23606

④ Ans: **Defining the action of S4 on-2 element subsets:**

The symmetric group S4 consists of all permutations of the set $x = \{1, 2, 3, 4\}$ we define an action of S4 on the set of 2-element subsets of x as follows:

for any σ S4 and any subset $\{a, b\}$ where $a, b \in X$ and $a \neq b$ define,

$$\sigma \cdot \{a, b\} = \{\sigma(a), \sigma(b)\}$$

Proving the action is well defined:

To show that this action is well defined, we must verify,

① The image of a-2 element subset under any permutation is until a 2-element subset.

② The identity element of S4 acts trivially.

③ The composition of two permutations become as expected.

closure: If $\{a, b\}$ is a 2-element subset of X. then for any $\sigma \in S4$ $\sigma(a) \neq \sigma(b)$ because σ is a bijection. Hence $\sigma \cdot \{a, b\} = \{\sigma(a), \sigma(b)\}$ is still a.2-element subset.

IT-23606

5) ans: We are given the finite field $GF(2^2)$ which is constructed using the irreducible polynomial

$$x^2+x+1$$

constructing $GF(2^2)$.

Since $GF(2^2)$ is a degree-2 extension of $GF(2)$ we define an element as a root of the irreducible polynomial

$$\alpha^2+\alpha+1=0$$

$$\alpha^2 = \alpha+1$$

since $GF(2) = \{0, 1\}$ we construct the elements of $GF(2^2)$ as:

$$GF(2^2) = \{0, 1, \alpha, \alpha+1\}$$

we know consider the non zero elements :-

$$E = \{1, \alpha, \alpha+1\}$$

① Closure: we compute the product:

$1.\alpha = \alpha.1$, $(\alpha+1) = \alpha+1$ and $1.1 = 1$

$\alpha(\alpha+1) = \alpha^2+\alpha = (\alpha+1)+\alpha = 1$

$(\alpha+1)(\alpha+1) = \alpha^2+2\alpha+1 = (\alpha+1)+2\alpha+1$

$= \alpha.\alpha = \alpha^2 = \alpha+1$

Since all products remain in E closure holds.

IT-23606

(6) Ans: Define the General Linear Group $GL(2,R)$:

The General Linear group $GL(2,R)$ consists of all 2×2 invertible matrices over:

$$GL(2,R) = \{A \in M_{2\times2}(R) \mid \det(A) \neq 0\}$$

This is a group under matrix multiplication.

Define the set of Scalar matrices:-

A scalar matrix is a multiple of the identity matrix.

$$S = \{\lambda I \mid \lambda \in R^*\} = \{\lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mid \lambda \neq 0\}$$

since λI is invertible for all $\lambda \neq 0$.

constructing the factor group:

The quotient group $GL(2R)$ consists of costs as the form:

$$[A] = AS = \{A(\lambda I) \mid \lambda \neq 0\}$$

since λI sealr all the element uniformaly, two matrices A and B belong to the same coset if and only if they differ by a sealr multiple:

$$A \sim B \iff B = \lambda A \text{ for some } \lambda \neq 0$$

This means that the cosets represent equivalence classes of matrices under

IT-23606

⑦ **Ans:** Difference Hellman key Exchange Protocol

The Diffie-Hellman (DH) key exchange is a cryptographic protocol that allows two parties to securly eastablish a shared secret over an inseeure channel without directly transmitting the secret itself.

Steps of the protocol:-

1. public parameters selection.
2. key exchange btn two parties.
3. Shared secret computation.

Potential Attacks and Defenses:

1. **Man in the middle attack:**

Attack: An attacker intercepts messages and establishes separate key exchanges with Alice and bob

Defense: use authenticated key exchange to verify.

2. **Brute force on pre computation Attacks:**

Attack: If the Prime p is small an attacker can precompute logarithms for all value.

Defense: use large primes to prevent of such attack.

CamScanner

IT-23606

⑧ Ans: Proof: Let G be a group and let H and K be two subgroups of G. we want to show that the intersection $H \cap K$ is also a subgroup

Step 1: show $H \cap K$ is non-empty since H and K are subgroups, they both contain the identity element e of G $e \in H$ and $e \in K$

Step 2: closure under multiplication:
let $a, b \in H \cap K$
since both H and K are subgroups, they are closed under multiplication, so.

$ab \in H$ and $ab \in K$

Thus $ab \in H \cap K$ proving closure under multiplicat

example:
consider the group of integers under addition $G = Z$ and let

$H = 2Z = \{ \ldots -4, -2, 0, 2, 4 \ldots \}$

$K = 3Z = \{ \ldots -6, -3, 0, 3, 6 \ldots \}$

The intersection $H \cap K$ consists of all integers that are both even and divisible 3 and 6

$H \cap K = 6Z = \{ \ldots -12, -6, 0, 6, 12 \ldots \}$

$6Z$ is a valid subgroup of Z.

IT-23606

(10) Ans: vulnerable of the DES cipher:-

The Data Encrypher standard developed in the 1970s was one of the most widely used symmetric encrypt algorithms, How ever due to advancement in compu power and analysis. DES is now considered insecure for modern application.

① short key length.
② Brute force attack
③ cryptanalytic weakness
④ small block size.

Brute force Attack Break DES:-

A brute force attack ~~break~~ systematically tries all possible keys until the correct is found
→ with 56-bit key there are $2^{56} \approx 72 \times 10^{-15}$ possible keys.

→ modern hardware, such as ASICs, FPGAs, and cloud based parallel processing can exhusted this key

AES Addressed the short coming DES:

The Advanced Encryption standard (DES) was introduced in 2001 to replace DBS and overcome is weakness.
→ Increased the key size.
→ Large block size.

IT-23606

(11) Ans: Differential cryptanalysis is a chosen plain text attack that analyze how difference in plaintext propagate through a cipher to predict differences in ciphertext.

Defense mechanisms in DES Against DC:-

1. S-Box Design to resist DC:

The S-boxes in DES were carefully designe to minimize differential probabilities

2. Feistal structure Provides:

In this Feistal network of DES, the right half of the block is expanded, mixed with the round key,

ii) Unlike DES, AES is not a Feistal cipher but follows a substitution - permutation structure to DC.

Key features that improve DC resistance:

i) substitutes
ii) shiftrows
iii) mix column for strong Diffusion.
iv) Add round key
v) more round in AES as AES-128 has 10 rounds.